Requirements and Procedures for the Exchange of Electronic Information with the Social Security Administration

Lisa J. Bryan, Chief Security Officer

Amber L. Daugherty, Assistant General Counsel

Created March 2017

Social Security Administration Federal Standards

- SSA must maintain oversight of the protected information it provides to the Department of Mental Health and utilized by department employees and contractors.
- All DMH employees, contractors, and agents who access SSA-provided information must be trained as to the sensitivity and protection of SSA-provided information.
- The DMH and its contractors are subject to and must comply with the Federal Information Security Management Act (FISMA), as part of the Electronic Government Act of 2002, and relevant policy issued by the National Institute of Standards and Technology (NIST) when accessing or using SSA-provided information.

What is protected SSA-Provided Information?

- SSA-provided information is used to verify and add client information in CIMOR.
- It will include personally identifiable information (PII) - information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with another personal or identifying information linked or linkable to a specific individual.
- Examples include: date and place of birth, mother's maiden name, and father's surname.

Safeguard of SSA-Provided Information

- DMH employees and contractors must protect SSA-provided information with efficient and effective security controls.
- DMH employees and contractors must only use SSA-provided information for a legitimate work purpose.
- Viewing and copying of SSA-provided information for a non-work purpose is prohibited.
- DMH employees and contractors are responsible for the proper use and protection of SSA-provided information.
- SSA-provided information shall be disposed of properly.
- A breach or loss of SSA-provided data shall be immediately reported to a local DMH Privacy or Security Officer.
- DMH employees and contractors shall be aware of procedures to protect the network from malware attacks, spoofing, phishing and pharming, and network fraud prevention.
- Misuse of SSA-provided information may lead to criminal, administrative, and civil sanctions, contract termination, and/or employee discipline.

CIMOR Access

- By accessing CIMOR, DMH employees and contractors are acknowledging that he/she will abide by all relevant federal laws, restrictions on access, use, disclosure, and the security requirements contained within the department's agreement with SSA.
- A copy of the SSA agreement and related documents are available on the CIMOR portal for review.